UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE META PIXEL TAX FILING CASES

Case No. 22-cv-07557-PCP

ORDER DENYING MOTION TO DISMISS

Re: Dkt. No. 183

In this consolidated putative class action against defendant Meta Platforms, Inc., plaintiffs filed an amended complaint that included a new claim alleging that the Meta Pixel operates as a pen register prohibited by the California Invasion of Privacy Act (CIPA). This Court previously held that plaintiffs had plausibly stated a claim that the Pixel is an unlawful wiretap under CIPA. Meta now moves to dismiss plaintiffs' new claim, arguing that plaintiffs have failed to state a pen register claim both because Meta does not "use" or "install" the Meta Pixel and because the Pixel cannot be both a wiretap and a pen register. For the reasons stated herein, Meta's motion is denied.

BACKGROUND

Meta operates the social network Facebook.[1] It makes money by selling ads. Part of Meta's value proposition is its ability to target users: Meta catalogs users' names, birthdays, genders, locations, contact information, and communications, as well as technical identifiers like IP addresses and device IDs. Meta assembles the information it collects about individual users and draws inferences to uncover attributes like "interests," "behavior," and "connections." Meta then offers advertisers the ability to target ads based on this data.

[1] For the purposes of Meta's Rule 12(b)(6) motion, the Court assumes the truth of the allegations in plaintiffs' second amended consolidated class complaint.

Meta has developed a tool called the Meta Pixel that third-party web developers can install on their sites. On the back end, the Pixel is a snippet of JavaScript code that loads a library of functions which developers can use to track actions users take on their sites. The Pixel logs these user actions and sends them to Meta, where developers can use and analyze the data, such as by measuring how effective their ads are or defining custom audiences for ad targeting. Every time the Pixel logs an action on a third-party website, the Pixel sends the data to Meta. Meta then attempts to match the action to one of its own users. If a user is logged into Facebook when visiting a third-party site, web cookies allow Meta to link the data transmitted by the Pixel directly to that specific user's Facebook account. If the Pixel data includes personal information like a name or email, Meta can also use that to perform a match. In addition to the utility offered to third-party developers, the Pixel benefits Meta, which amasses the data collected by the Pixel into detailed "dossiers" that it keeps for registered Facebook users and non-users alike. This data, in turn, is used to target ads based on individuals' interests and activity, including their activity on non-Meta products. Meta offers other tools to developers that work similarly, including the Facebook SDK (which allows advertisers to track user actions on mobile apps) and the Conversion API (which allows developers to track actions taken by users who have opted out of tracking).

H&R Block, TaxAct, and TaxSlayer are widely used services for filing taxes online. These services installed the Pixel and other Meta tracking tools on their websites. As a result, the tracking tools transmitted financial information about the tax sites' users to Meta, including names, email addresses, and data about income, filing status, refund amounts, and dependents' college scholarship amounts. In particular, plaintiffs allege that TaxAct sent its users' filing status, adjusted gross income, and refund amount to Meta; that H&R Block transmitted data about health savings accounts and college tuition grants and expenses; and that TaxSlayer transmitted phone numbers and names, including of dependents. Plaintiffs allege that Meta's tracking tools link specific users to the tax-related information sent by TaxAct, H&R Block, and TaxSlayer. The Pixel also transmit webpage URL data from the tax filing websites to Meta. This data discloses specific issues about which the users of the websites have inquired. For example, one user

inquired with H&R block whether they could "claim[] a boyfriend on taxes," and the Pixel then transmitted to Meta that a given user had visited the following URL: https://www.hrblock.com/tax-center/filing/dependents/claiming-boyfriend-on-taxes/. The Pixel transmitted thousands of similar URLs to Meta, revealing the putative class members' inquiries about matters such as COVID-19, lotteries, and obtaining loans.

As relevant here, the plaintiffs in this case allege that the Pixel sent this data to Meta from the TaxAct, H&R Block, and TaxSlayer websites. They contend that this violates the provision of CIPA that prohibits installing a wiretap without the consent of all parties to a communication. *See* Cal. Penal Code § 631. On May 9, 2025 plaintiffs filed a second amended consolidated class complaint which further asserts that the Pixel violates the provision of CIPA that prohibits installing a pen register without a court order. *See id.* § 638.51. Plaintiffs contend that the Pixel is a pen register because it "is a device or process that records or decodes dialing, routing, addressing, or signaling information from the electronic communications transmitted to or from subject tax filing websites." Meta now moves to dismiss plaintiffs' pen register claim under Rule 12(b)(6).

LEGAL STANDARDS

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include a "short and plain statement of the claim showing that the pleader is entitled to relief." Under Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon which relief can be granted. Dismissal is required if the plaintiff fails to allege facts allowing the Court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "Dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To survive a Rule 12(b)(6) motion, a plaintiff need only plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

In considering a Rule 12(b)(6) motion, the Court must "accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable" to the non-moving party.

Rowe v. Educ. Credit Mgmt. Corp., 559 F.3d 1028, 1029–30 (9th Cir. 2009). While legal conclusions "can provide the [complaint's] framework," the Court will not assume they are correct unless adequately "supported by factual allegations." *Iqbal*, 556 U.S. at 679. Courts do not "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

ANALYSIS

Pursuant to Section 638.51(a) of the California Penal Code, "a person may not install or use a pen register … without first obtaining a court order[.]" A pen register is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code. § 638.50(b). Meta makes two arguments in support of its motion to dismiss. First, Meta argues that the complaint fails to allege facts showing that Meta either "install[ed] or use[d]" the Pixel. Second, Meta argues that because the complaint alleges that the Pixel discloses the "contents of communications" between users and the tax websites, the plaintiffs have effectively pleaded themselves out of their pen register claim.

I. The complaint makes plausible allegations that Meta "used" a pen register.

Meta argues that the complaint fails to plausibly allege that Meta either installed or used the Pixel, which is necessary to state a claim under Section 638.51. Because the complaint adequately alleges that Meta used the Pixel, the Court need not address whether the complaint sufficiently alleges that Meta installed the Pixel.

The central thrust of Meta's argument is that CIPA imposes liability for *using* a pen register but not for *using data received from* a pen register. In Meta's view, it is the tax websites who both install and use the Pixel while Meta, by contrast, merely uses the data that it receives from the Pixel without using the Pixel itself. In support of its argument, Meta points to textual differences between CIPA's pen register and wiretap provisions. Whereas CIPA imposes liability on any person who unlawfully "uses, or attempts to use," information obtained from a wiretap, CIPA's pen register provisions include no such prohibition. Cal. Penal Code § 631(a). Meta notes

a similar distinction in the analogous federal statutes. *Compare* 18 U.S.C. § 2511(b) (imposing liability on individuals who "use … the contents" of illegally obtained communications), *with* 18 U.S.C. § 3121(a) (imposing liability only on individuals who "install or use a pen register").

The problem with Meta's argument is that the complaint clearly asserts that Meta uses the Pixel. Plaintiffs generally allege that Meta provides the Pixel to the tax services who then install the Pixel on their websites. The Pixel tracks user activity on those websites and, as it tracks that activity, it "transmit[s information] in real time to Meta's servers in California, where the information is stored." SAC ¶30. Indeed, the complaint is replete with allegations that Meta uses the Pixel to intercept data sent between the user and the tax websites and transmit that data back to its own servers. It is only after Meta has received that information from the Pixel that it can use that data to provide third-party websites with Meta's analytics services. Whether or not Meta's mere use of the data generated from the Pixel violates Section 638.51, the complaint adequately alleges that Meta is using the Pixel to record and transmit that data to its servers in order to enable the Pixel's core value proposition.

Meta's attempt to distinguish using the Pixel from using data collected by the Pixel might be more principled if, for example, the complaint alleged that the tax services collected data and then sent that data to Meta themselves. But the complaint instead alleges that the tool Meta admittedly created sends data to Meta in real time without any intervening actor breaking the chain of transmission. The complaint alleges that Meta receives some information from the Pixel before the tax services themselves receive the data.[2] For certain "high-traffic websites," Meta even "employs account managers to help website developers and owners use the Meta pixel" in return for significant ad revenue. SAC ¶80. Thus, the complaint plausibly alleges that Meta used the Pixel to collect user data.

Unable to avoid plaintiffs' allegations, Meta relies instead upon a shaky analogy. It states

[2] To be sure, the complaint often states that the Pixel transmits the contents of communication in real time. But plaintiffs have also alleged that the Pixel collects the sort of "dialing, routing, addressing, or signaling information" encompassed within Section 638.50(b), which Meta does not dispute. Plaintiffs are therefore entitled to the inference that the Pixel transmits that "dialing, routing, addressing, or signaling information" data in real time as well.

that while a police officer may be held liable under Section 638.51 for installing or using a pen register without a court order to identify phone numbers called by the suspect of an investigation, Meta is more like the prosecutor who subsequently uses the data collected by a pen register to initiate a prosecution. Meta argues that the prosecutor cannot be held liable for using that data to later prosecute the suspect. But this analogy supplies only half of the picture painted by the complaint. A more apt example derived from plaintiffs' allegations would involve a prosecutor who purchased a pen register, handed that pen register to a police officer and then instructed the police officer to install it without a court order and further aided the officer in doing so. If the prosecutor then used the pen register to collect phone numbers in real time—whether or not the prosecutor later used those phone numbers to prosecute a suspect—the prosecutor would have "used" the pen register under the plain terms of the statute. The fact that the complaint alleges that the Pixel allows Meta to collect data in real time in order to provide third-party websites with the analytics services that flow from installation of the Pixel defeats any notion that Meta does not itself use the Pixel for the purposes of Section 638.50(b).

The complaint therefore plausibly alleges that Meta used a pen register.

II. The Pixel's disclosure of the contents of communication does not preclude it from also being a pen register.

Meta next argues that plaintiffs have pleaded themselves out of a pen register claim. CIPA defines a pen register as a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, *but not the contents of a communication.*" Cal. Penal Code. § 638.50(b) (emphasis added). In Meta's view, the central theory of plaintiffs' lawsuit is that the Pixel is a wiretap because it collects the contents of communications. Meta argues that plaintiffs cannot have it both ways and that, by including the language "but not the contents of a communication" in its definition of a pen register, CIPA precludes a device from being both a pen register and a wiretap.

The relevant statutory language is ambiguous. On the one hand, that language could be interpreted, as Meta contends, to define a pen register as a device that records *only* "dialing,

routing, addressing, or signaling information" and that does *not* record "the contents of a communication."[3] On the other hand, it could be interpreted to define a pen register as any device that records "dialing, routing, addressing, or signaling information" while clarifying that a device that records *only* "the contents of a communication" is not a pen register, and is instead subject solely to CIPA's wiretap provisions. The statute does not, through its language alone, clarify whether it establishes two entirely nonoverlapping zones of regulation, as Meta contends, or whether a device that collects wiretap content and pen register metadata is subject to *both* CIPA's wiretap provisions and its pen register provisions.

In the absence of a conclusive basis in the text for resolving such a matter of statutory interpretation, California courts "determine the Legislature's intent so as to effectuate the law's purpose." *Skidgel v. Cal. Unemp. Isn. Appeals Bd.*, 12 Cal. 5th 1, 14 (2021) (citation omitted); *see People v. Cole*, 28 Cal. 4th 964, 975 (2006) ("If, however, the language supports more than one reasonable construction, then we may look to … the ostensible objects to be achieved and the legislative history."). Here, there is no doubt that the California Legislature, in enacting CIPA, intended "to protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties that cannot be tolerated in a free and civilized society. This philosophy appears to lie at the heart of virtually all the decisions construing [CIPA]." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (cleaned up). Recognizing this intent, the California Supreme Court "has instructed courts to interpret CIPA in the manner that 'fulfills the legislative purpose of CIPA by giving greater protection to privacy interests.'" *Matera v. Google, Inc.*, 15-cv-04062-LHK, 2016 WL 8200619, at *19 (N.D. Cal. 2016) (quoting *Flanagan*, 27 Cal. 4th at 775).

Given CIPA's purpose to protect Californians' privacy, it is highly unlikely that the Legislature intended to permit the installation and use of pen registers so long as those devices

[3] Because Meta has not moved for dismissal on that basis, the Court assumes without deciding that the complaint plausibly alleges that the Pixel records "dialing, routing, addressing, or signaling information" that has been "transmitted by an instrument or facility from which a wire or electronic communication is transmitted[.]" Cal. Penal Code § 638.50(b).

also record the contents of a third party's communications. Under Meta's interpretation of the statute, an entity could escape liability under CIPA's pen register provisions by combining the functionality of a wiretap with that of a pen register. That entity could also escape liability under CIPA's wiretap provisions by utilizing only the information tracked by pen registers and not "read[ing], or attempt[ing] to read ... the contents" of communication. Cal. Penal Code § 631(a). Such an entity could engage in the very conduct that CIPA proscribes—using a pen register without a court order—while escaping liability through a statutory loophole that is available only because that entity collects even more sensitive information (the content of Californians' communications) along with the information recorded by pen registers. In contravention of the California Legislature's intent in enacting CIPA, Meta's proposed loophole would allow any entity to avoid CIPA's pen register provisions simply by employing more intrusive forms of technology.

The Court raised this concern at the hearing on Meta's motion, and Meta replied that the statute was in fact intended to operate in this precise manner. Meta notes that Section 638.51(b) provides an exception to 638.51(a)'s command that a "person may not install or use a pen register … without first obtaining a court order" by allowing a "provider of electronic or wire communication service [to] use a pen register" without first seeking a court order in a narrow set of circumstances related to running their network and providing customer service. In Meta's view, Section 638.50(b)'s exclusion of "the contents of communication" from the definition of pen register is intended to clarify that telecoms cannot install an authorized pen register that operates as a shadow wiretap. According to Meta, installing a device that collects the contents of communications deprives the offending telecom entirely of the pen register exception and instead subjects it to CIPA's wiretap provisions.

Meta's argument, however, would effectively render Section 638.51(b)'s telecom exception superfluous. If Meta is correct that any entity can install a pen register that also collects the contents of communication without facing liability under CIPA's pen register provisions, why would Section 638.51(b) exist at all? A telecom could install a pen register to collect metadata for the purposes clearly enumerated within subsection (b)—such as to protect its own rights or

property—but if it were also using that device to collect the contents of communications, Section 638.51(a)'s court order requirement would not apply and there would be no need for an exception. More troubling still, a telecom could install a pen register to collect data for purposes that do not fall within subsection (b)'s enumerated exceptions—such as for advertising purposes—but if that same entity also used the device to record the content on its customers phone calls, the telecom could install the pen register without the court order required by Section 638.51(a).

Although Meta expresses concern about an authorized pen register masquerading as a shadow wiretap, its argument would allow an *unauthorized* pen register to circumvent judicial oversight so long as that device included a modicum of nonessential wiretapping technology. Because recognizing such a loophole would significantly limit the privacy protections offered by CIPA's pen register provisions, it is unsurprising that courts regularly allow both wiretap and pen register claims to proceed. *See Zarif v. Hwareh.com, Inc.*, 23-cv-0565-BAS-DEB, 2025 WL 486317 (S.D. Cal. Feb. 13, 2025); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023); *Moody v. C2 Educ. Sys. Inc.*, 742 F. Supp. 3d 1072 (C.D. Cal. 2024). Given CIPA's purpose to protect Californians against the privacy intrusions that can result from either wiretaps or pen registers, the better interpretation of Section 638.51 is that it defines a pen register as any device that "records dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," but not a device that records only "the contents of communications." Under this construction of the statute, Meta's argument that plaintiffs fail to plead its use of a pen register without a warrant fails.

In any event, even assuming Meta were correct that CIPA precludes a single device from being both a wiretap and a pen register, its motion would still fail. The complaint alleges that the Pixel is a "small library of functions" with an array of capabilities that allows the website owner to do a variety of things. SAC ¶27. One of those functions collects data such as "HTTP Headers" and IP addresses, while a different function collects the contents of users' communications. If the various functionalities within the Meta Pixel operate independently from one another, as plaintiffs plausibly allege, the process that records metadata in a pen register-like manner is a separate "device" or "process" from the one that collects the contents of users' communications. Under

Section 638.51, plaintiffs are entitled to pursue a claim against Meta for its use of the pen register "device" without a warrant whether or not Meta has also installed or used a separate wiretap device to record and review the contents of users' communications.

CONCLUSION

For the reasons stated herein, Meta's motion to dismiss plaintiffs' pen register claim is denied.

IT IS SO ORDERED.

Dated: August 6, 2025

P. Casey Pitts
United States District Judge